Background information:

Glossary of Internet terms

Administrator

Person with unlimited access to all features of a local network; responsible for the administration and maintenance of the network. Among other tasks, the administrator assigns IP addresses within the network and must ensure that they are unique.

ARP - Address Resolution Protocol

ARP is used for the mapping of IP addresses to the respective Ethernet address of a network participant. The detected assignments are administered in the ARP table of each individual computer. In Windows systems, you have the option to modify the ARP table using the ARP command.

Properties and parameters of the ARP command in the DOS window:
ARP -A lists the entries in the ARP table
ARP -S <IP-Adresse> <Ethernet-Adresse> adds a static entry to the ARP table
ARP -D <IP-Adresse> deletes and entry from the ARP table
ARP is defined in the RFC-826 Internet standard.

Bridge

Bridges connect subnetworks and determine, based on the Ethernet address, which packets are to pass the bridge and which are to be refused. The respective information is retrieved from the bridge tables. Depending on the bridge type, this data must be manually entered by the administrator or is generated dynamically by the bridge.

See also Router

Broadcast

A broadcast is an all-call to all network stations. A typical broadcast application is the ARP-request. However, other protocols - such as RIP - use broadcasts, too.

Broadcasts are not sent through routers or bridges.

Client

Workstations or applications that establish connections to servers to employ the respective services. The best known client is the web browser that connects to a web server. Basically all Internet services such as e-mail, FTP, Telnet, socket, etc. apply the client/server architecture.

The client is thereby the "caller", while the server expects the "calls" to answer them.

Client/server architecture

Systems with "distributed intelligence", where a client establishes a connection to a server to avail of its services. Certain server applications are able to simultaneously serve multiple clients.

Com-Servers

Small terminal devices in TCP/IP-Ethernet networks, providing interfaces for serial devices and digital I/O ports via the network. Com-Servers can be used as servers or clients respectively.

DHCP - Dynamic Host Configuration Protocol

Dynamic, temporary assignment of IP addresses from an address pool.
DHCP is used to automatically configure TCP/IP networks. The configuration does therefore not require any manual modifications and is carried out centrally and thus consistently. The system administrator defines how the IP addresses are to be assigned and specifies the period of assignment.

This procedure basically results in a system where each network station is assigned a new IP address each time a connection is established. Therefore, network components such as Com-Servers or print server that are always accessed via a specific IP address must be excluded from the IP address assignment by means of DHCP.

DHCP is defined in the RFC 2131 (03/97) and RFC 2241 (11/97) Internet standards.

DNS - Domain Name Service

Network stations on the Internet are accessed via numerical IP addresses. However, as names can be better remembered than numbers, the DNS system was introduced.
When a domain name is entered by the user, the TCP/IP stack queries the next DNS server for the associated IP address. The DNS server manages a list in which the IP addresses of the network or the domain are assigned to the respective host names.

Example of a DNS table:
172.16.232.10 webtherm.firma.de

172.16.232.11 ntsrv.firma.de
172.16.232.12 novellsrv.firma.de
...

If the user or application requests a connection to participant "Htsrv", the request is initially transferred to the DNS server, which returns the IP address 172.16.232.11 for the host name. The same procedure is applied on the Internet. The Internet DNS servers however contain URLs, e.g. klima.wut.de. If the requested host name is not included in the table of the DNS server, the request is sent to the next DNS servers in the network. If, after a certain time, no reply is received from any of the queries DNS servers, the connection is terminated and the web browser shows and error message, indicating that the page has not been found.

DNS is based on a hierarchical logic: each name is initially identified by a top-level domain (e.g. "de", "com", "net", etc.) and a sub level domain. Each sub level domain may contain additional subordinate domains. The individual name sections identifying the levels are separated by full stops.

Network resources should possibly be assigned a domain name that is directly related to the services on offer or that includes the company name of the service provider. Example: "WuT.de" is in the top-level domain" de" (= Germany) and the sub level domain "WuT" (= Wiesemann & Theis GmbH).

DNS server

DNS servers are part of the Internet and provide a service where domain names are "translated" into IP addresses.

Ethernet

Ethernet is the currently most commonly used technology for local networks. There are three different Ethernet topologies: 10Base2, 10Base5 and 10BaseT; the transfer rate of Ethernets is 10 Mbit/s.

Ethernet address

Unchangeable physical address of a network component in an Ethernet.

Firewall

A firewall is a set of network components that, similar to a router, connect an internal network (intranet) to a public network (e.g. Internet). Access to the other network can thereby be limited or fully blocked, depending on the access direction, the service used and the identification of the network station or user.

Firewalls may also include the encryption of data, for example if the public network is only used as a transfer route between two geographically separated intranets.

FTP - File Transfer Protocol

FTP is an upper-level TCP/IP that allows for the transfer of entire files between two network stations. FTP, like all other TCP protocols, applies the client/server method. The FTP client thereby initiates the procedure, and the parameters, type and direction of the data transfer are forwarded to the server together with the FTP command sent by the user.

After the FTP command has been entered DOS window
FTP <IP-Adresse des FTP-Servers>
the client initially establishes a connection to the FTP server, which in turn requests the user name and a password, if applicable.

As soon as the connection is established properly, access to the FTP server is possible by means of other commands and parameters. Examples:
ascii switches to the transmission of text files
binary switches to the transmission of binary files
put <Dateiname> sends the specified file to the FTP server
get <Dateiname> reads the specified file from the FTP server
In addition to the above commands, FTP in Windows offers a range of other options. For more information, refer to the DOS help file (Enter "?" at the FTP prompt). The syntax of the FTP commands vary between operating systems.

FTP is described in detail in RFC 959.

Gateway

Gateways, like **bridges** and **routers** , connect different networks with each other. While bridges and routers thereby connect the physical types of the networks (e.g. Ethernet - ISDN) and thus do not affect the actual protocol (e.g. TCP/IP), gateways allow for access to networks controlled by different protocols (e.g. from TCP/IP to profibus). A gateway is thus able to "translate" between different communication protocols.

Please note: When configuring networks in Windows systems, the entry of a gateway is mandatory. This entry however refers to routers that are already installed in the network!

ICMP - Internet Control Message Protocol

The ICMP protocol is used to transmit status information and error messages between the IP nodes. ICMP also allows for echo requests to establish whether a destination is available.

See also Ping

Internet

The Internet is the world's largest association of networks, allowing users to use a virtually unlimited infrastructure for communication. By the use of TCP/IP, network users can avail of Internet services such as e-mail, FTP, and browsers (HTTP, etc.).

Intranet

A non-public network (e.g. within a company), providing users with Internet-like services such as e-mail, FTP, or HTTP browsing within the network.
Most intranets are equipped with routers and firewalls providing access to the Internet.

IP - Internet Protocol

Protocol that allows users to communicate with partners in other networks.

IP address

The IP address is a 32-bit numerical code that uniquely identifies each network station in the intranet or the Internet. It consists of a network code (net ID) and a host code (host ID).

ISDN - Integrated Services Digital Network

ISDN is the new standard of the telecommunications technology and has replaced the analog telephone network in Germany and other countries. ISDN integrates a number of services such as telephone, fax but also video conferencing and data transfer into one system. Therefore, ISDN is suitable for the transfer of voice, text, graphics and other digital data from one terminal device to an other.
Through the S0 interface of a basic connection, ISDN provides two basic channels (B channels) at 64kbit/s each and a control channel (D channel) at 16kbit/s. The digital connection to the end user has thus a combined transfer rate of 144kbit/s (2B+D). The two B channels can be used simultaneously for two different services at a bit rate of 64kbit/s.

ISDN router

ISDN routers allow for the communication between two local networks via the ISDN network of the telephone system provider. ISDN routers thereby act as normal routers but also handle the ISDN connection.

LAN - Local Area Network

Local network within a defined area, using a fast transmission medium such as Ethernet.

MAC ID

Not modifiable, physical address of a network component (MAC = Media Access Control).

See also Ethernet address

NAT - Network Address Translation

Due to the huge growth of the Internet over the past few years, a shortage of IP addresses has occurred, so that they are today only assigned sparingly. NAT is used where internal networks of companies are connected to the Internet. The intranet is linked through a NAT-capable router to the Internet, while internally, IP addresses that are not relevant to the Internet are used. In this case, the network is accessible from outside via one single (or a few) IP address(es). Based on the port number in the received TCP/IP packet, this packet is routed to a specific internal network station.

Example: The address klima.wut.de is dissolved by the DNS server of the provider and the request is sent to the respective IP address. When the request reaches the ISDN router this IP address is routed by means of NAT to the internal IP address of the W&T Web Thermometer, thus enabling the access to the device.

Ping - Packet Internet Groper

Ping is used in TCP/IP networks for diagnostic purposes; with this feature, it is possible to establish whether a specific station is actually part of the network and accessible. Ping uses the ICMP protocol, which in turn is based on the IP protocol. When a network station issues an ICMP request by entering the ping command, the respective station sends an ICMP reply back to the sender.
The command PING <IP-Adresse> entered in the DOS window, requires the station with the respective IP address to send a reply.

The following parameters can be entered in addition to the IP address:
-t Repeats ping command in a loop until the user terminates the command with <Ctrl>C.
-n count Repeats the ping command "count" times.
-l size "Size" indicates the number of bytes included in the ICMP packet. For Com-Servers the default settings are max. 512 bytes.
-w timeout "Timeout" specifies the period (in milliseconds) during which the station waits for a reply.
Example:
PING 172.16.232.49 -n 50
repeats the ping command to station 172.16.232.49 fifty times.

A reply from a network station looks like this:
Reply from 172.16.232.49: bytes=32 time=10ms TTL=32

If no reply is issued, the following message is returned:
Request timed out.

The ICMP packets used for ping are defined in the RFC-792 Internet standard.

PPP - Point to Point Protocol

PPP is an enhanced successor of **SLIP** and features improved error correction, etc.

Like SLIP, PPP allows TCP/IP devices that have no LAN connection to participate in TCP/IP networks over the serial interface.

RIP - Routing Information Protocol

Routing protocols such as RIP are used to exchange information on changed routes between two networked systems, allowing for dynamic changes in the routing tables.

RIP is defined in the RFC-1058 Internet standard.

Router

Routers are used to connect networks of different type. In contrast to bridges, the decision on which data packets are to be forwarded is not based on Ethernet address but on IP address instead.

See also Bridge

Server

Workstations or applications that accept connections established by clients and make the requested services available to them. The best known server is the web server that provides data to a web browser. Basically all Internet services such as e-mail FTP, Telnet, sockets, etc. apply the client/server architecture.

The server expects "calls" to answer them, while the client is the "caller".

SLIP - Serial Line Internet Protocol

SLIP provides an easy option to transfer TCP/IP packets by means of serial point-to-point lines. This allows for the integration of terminal devices that are not equipped with a LAN connection in networks, using the serial interface.

SLIP operates a very simple algorithm without data integrity checking: the actual IP data packet is equipped with a preceding start character (decimal 192) and an end character (also decimal 192). To ensure binary transparency, the start and end characters contained in the data packet are thereby replaced by other sequences.

SLIP is described in detail in RFC 1055.

SLIP router

A SLIP router consists of the hardware and functionality for the integration of serial terminal devices that are equipped with a TCP/IP stack into the network.

Com-Servers offer SLIP routing as a mode option.

SNMP - Simple Network Management Protocol

SNMP is based on UDP and allows for the centralized administration and monitoring of the network components.

SNMP is specified in the following standards: RFC 1052, RFC 1155, RFC 1156, RFC 1157, RFC 1213 and RFC 1441.

Subnet mask

32-bit value, defining the sections of the IP address that refer to the network and the network station respectively.

TCP - Transmission Control Protocol

TCP is used in conjunction with IP and, firstly establishes the connection of the station during the data transfer, while it also checks the integrity of the data and sequence of the packets.

TCP/IP stack

Component of the operating system or of a driver containing all functions and drivers required for the support of the IP protocol.

Telnet - Terminal over Network

In the past, Telnet was mainly used for remote access to UNIX servers via the network. A Telnet application (Telnet client) allows remote access to any workstation in the network (Telnet server). Today, Telnet is also used for the configuration of network components such as Com-Servers. With TCP/IP, Telnet is normally accessed through port 23; for special applications, it is though possible to assign different port numbers. Telnet is used in conjunction with TCP/IP and works as a transfer and integrity protocol.

Properties and parameters of Telnet in the DOS window:
TELNET <IP-Adresse>
Establishes a Telnet connection to port 23 of the Telnet server with the respective IP address.

TELNET <IP-Adresse> <Port-Nr>
Establishes a Telnet connection to the entered port of the Telnet server.

Example: In order to establish a Telnet connection to the configuration port (1111) of a W&T Com-Server, the following command must be entered:
TELNET 172.16.232.49 1111

In a Windows environment, the address parameters for Telnet connections are entered in menu *Connect/Network system*. In the dialog field *Host name,* enter the IP address of the Telnet server; in *Connection,* enter the desired port number. The default entry *telnet* corresponds to port 23.

Telnet is defined in the RFC854 Internet standard.

TFTP - Trivial File Transfer Protocol

TFTP is an alternative to FTP for the transfer of files over networks. However, TFTP includes only a minimum number of commands and does not support comprehensive data integrity features. It uses UDP as the actual transfer protocol. As UDP is an unsecured protocol, minimal security features have been implemented in TFTP.

TFTP is described in detail in the standards 783, 906, 1350 and 1782 to 1785.

UDP - User Datagram Protocol

UDP is a protocol similar to TCP on IP. In contrast to TCP, it does not require a connection and includes no integrity check mechanisms. The advantage of UDP over TCP lies in its higher data transfer rate.

W&T
www.WuT.de

We are available to you in person:

Wiesemann & Theis GmbH
Porschestr. 12
42279 Wuppertal

Phone: +49 202/2680-110 (Mon.-Fri. 8 a.m. to 5 p.m.)
Fax: +49 202/2680-265
info@wut.de

Data Privacy